Targeted Attacks Against Civil Society in Asia

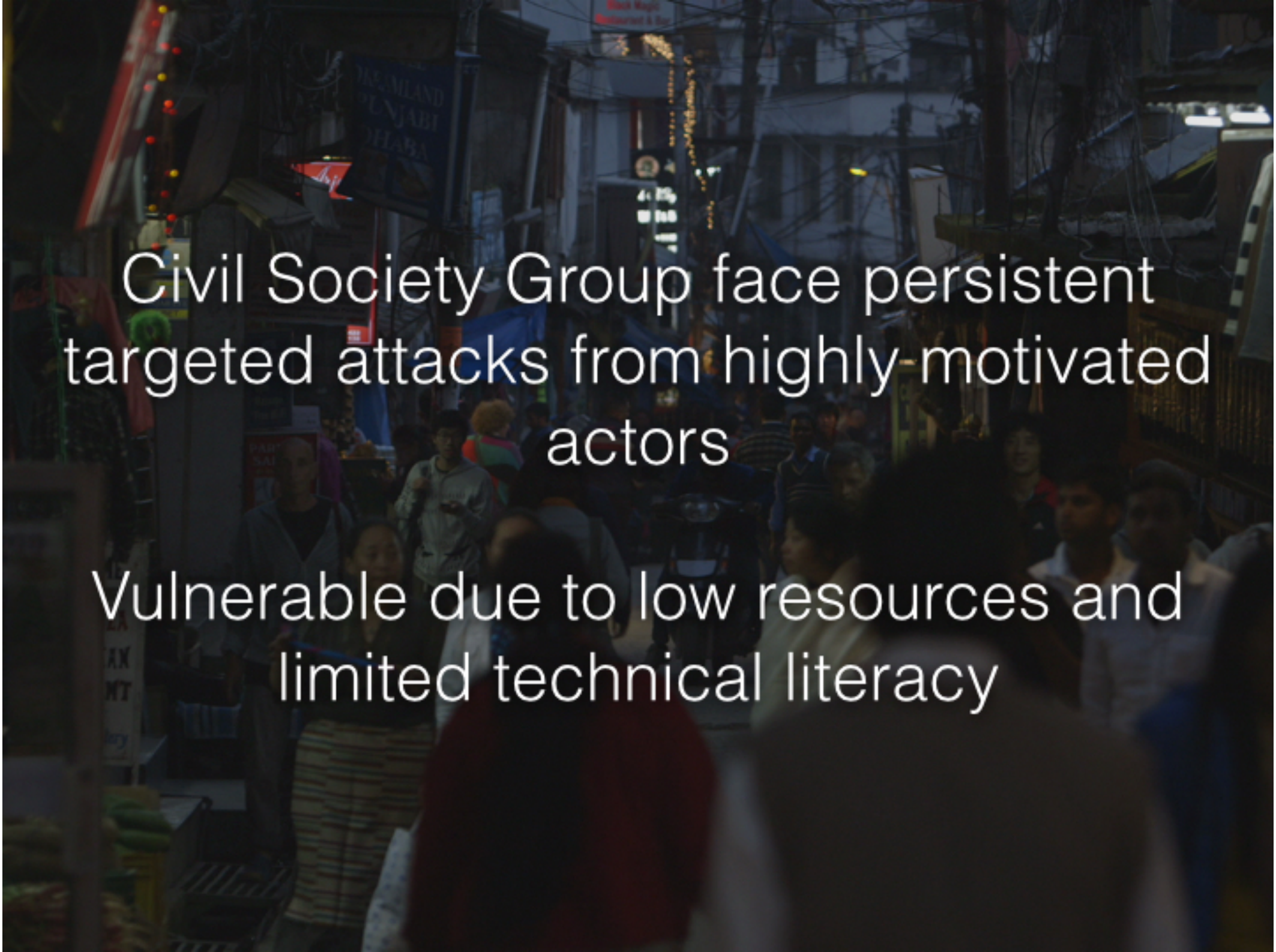
Or why you should check the md5 before opening this deck.

Katie Kleemola

Citizen Lab, Munk School of Global Affairs, University of Toronto

katie@citizenlab.org

HITB GSEC 2015


Civil Society Group face persistent targeted attacks from highly-motivated actors
Vulnerable due to low resources and limited technical literacy

Study of 10 civil society groups over 4 years

Report: https://targetedthreats.net

Indicators:
https://github.com/citizenlab/malware-indicators

Case Studies

Tibetan Diaspora

Hong Kong

Burma


Attacks on Tibetan Diaspora

From Wangpo Tethong <w.tethong1@yahoo.com>

Subject **Detailed arrangements: Proclamation of First European Declaration**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete

2015-03-10 11:40 PM

Dear Tibetan Media

Please find attached the Detailed arrangements about the Proclamation of First European Declaration for Tibet in Paris on March 14, 2015.

We have already translated the draft press releases and email sent to you, such as over the confiscation of related accessories to please reply to me as soon as possible.

More information can be found on www.europe-stands-with-tibet.org <hxxp://www.europe-stands-with-tibet.org/>

On behalf of the Working Committee for the "March 10th Rally" in Paris.
Wangpo Tethong

1 attachment: Detailed arrangements.doc 183.3 KB

From Wangpo Tethong <w.tethong1@yahoo.com>

Reply | Reply All | Forward | Archive | Junk | Delete

Subject Detailed arrangements: Proclamation of First European Declaration

2015-03-10 11:40 PM

To [redacted]

Dear Tibetan Media

Please find attached the Detailed arrangements about the Proclamation of First European Declaration for Tibet in Paris on March 14, 2015.

We have already translated the draft press releases and email sent to you, such as over the confiscation of related accessories to please reply to me as soon as possible.

More information can be found on www.europe-stands-with-tibet.org <hxxp://www.europe-stands-with-tibet.org/>

On behalf of the Working Committee for the "March 10th Rally" in Paris.
Wangpo Tethong

1 attachment: Detailed arrangements.doc 183.3 KB

From Wangpo Tethong <w.tethong1@yahoo.com>

Subject **Detailed arrangements: Proclamation of First European Declaration**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete

2015-03-10 11:40 PM

Dear Tibetan Media

Please find attached the Detailed arrangements about the Proclamation of First European Declaration for Tibet in Paris on March 14, 2015.

We have already translated the draft press releases and email sent to you, such as over the confiscation of related accessories to please reply to me as soon as possible.

More information can be found on www.europe-stands-with-tibet.org <hxxp://www.europe-stands-with-tibet.org/>

On behalf of the Working Committee for the "March 10th Rally" in Paris.
Wangpo Tethong

1 attachment: Detailed arrangements.doc 183.3 KB

From Wangpo Tethong <w.tethong1@yahoo.com>

Subject **Detailed arrangements: Proclamation of First European Declaration**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete

2015-03-10 11:40 PM

Dear Tibetan Media

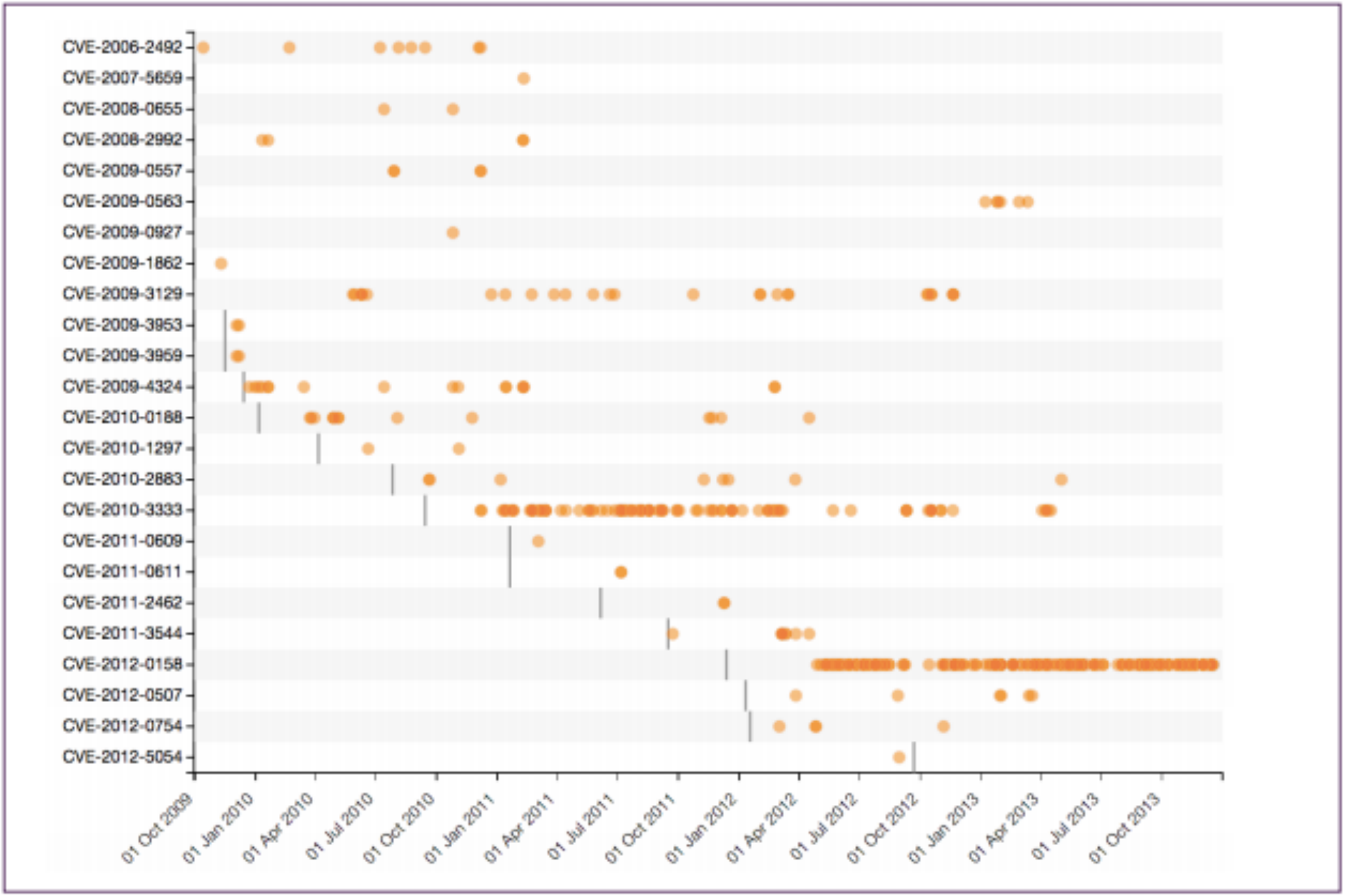
Please find attached the Detailed arrangements about the Proclamation of First European Declaration for Tibet in Paris on March 14, 2015.

We have already translated the draft press releases and email sent to you, such as over the confiscation of related accessories to please reply to me as soon as possible.

More information can be found on www.europe-stands-with-tibet.org <hxxp://www.europe-stands-with-tibet.org/>

On behalf of the Working Committee for the "March 10th Rally" in Paris.
Wangpo Tethong

1 attachment: Detailed arrangements.doc 183.3 KB


CVE-2006-2492
CVE-2007-5659
CVE-2008-0655
CVE-2008-2992
CVE-2009-0557
CVE-2009-0563
CVE-2009-0927
CVE-2009-1862
CVE-2009-3129
CVE-2009-3953
CVE-2009-3959
CVE-2009-4324
CVE-2010-0188
CVE-2010-1297
CVE-2010-2883
CVE-2010-3333
CVE-2011-0609
CVE-2011-0611
CVE-2011-2462
CVE-2011-3544
CVE-2012-0158
CVE-2012-0507
CVE-2012-0754
CVE-2012-5054
01 Oct 2009
01 Jan 2010
01 Apr 2010
01 Jul 2010
01 Oct 2010
01 Jan 2011
01 Apr 2011
01 Jul 2011
01 Oct 2011
01 Jan 2012
01 Apr 2012
01 Jul 2012
01 Oct 2012
01 Jan 2013
01 Apr 2013
01 Jul 2013
01 Oct 2013

From Net Tibet <tibet_net@yahoo.com.hk <mailto:tibet_net@yahoo.com.hk>>

Reply | Reply All | Forward | Archive | Junk | Delete

Subject **XI JINPING'S TIBET CHALLENGE (Details attched)**

2015-04-30 01:57 PM

To [redacted]

Dear,

Twenty four months ago Xi Jinping, and 5th generation leaders, inherited extraordinary powers as they took over the helm of the Chinese Communist Party. Alongside these powers they also took on a considerable number of major challenges, prominent among which is China's occupation of Tibet.

In this powerful new role Xi Jinping was given the opportunity to change four generations of failed Tibet policies by adopting a paradigm shift in the Chinese Communist Party's approach to Tibet that gives full agency over formulating future policies to the Tibetan people.

However Xi has shown no sign of changing course in Tibet. Instead the Chinese Communist Party can be seen to be continuing down the failed path of previous generations of Chinese leaders, implementing a harsh military crackdowns and unsustainable economic subsidies, which - far from bringing about the stability they seek - serve to exacerbate Tibetan grievances and create widespread resistance right across Tibet.

During the past 24 months we have seen China's stranglehold occupation in Tibet maintained by Three Pillars of Coercive Control: Military Occupation, Colonial Rule and Fear and Intimidation.

Xi Jinping needs to recognize that Tibetan resistance to China's failed Tibet policies is not fading away, and the growing strength of international condemnation of China's leadership is further highlighting the need for change.

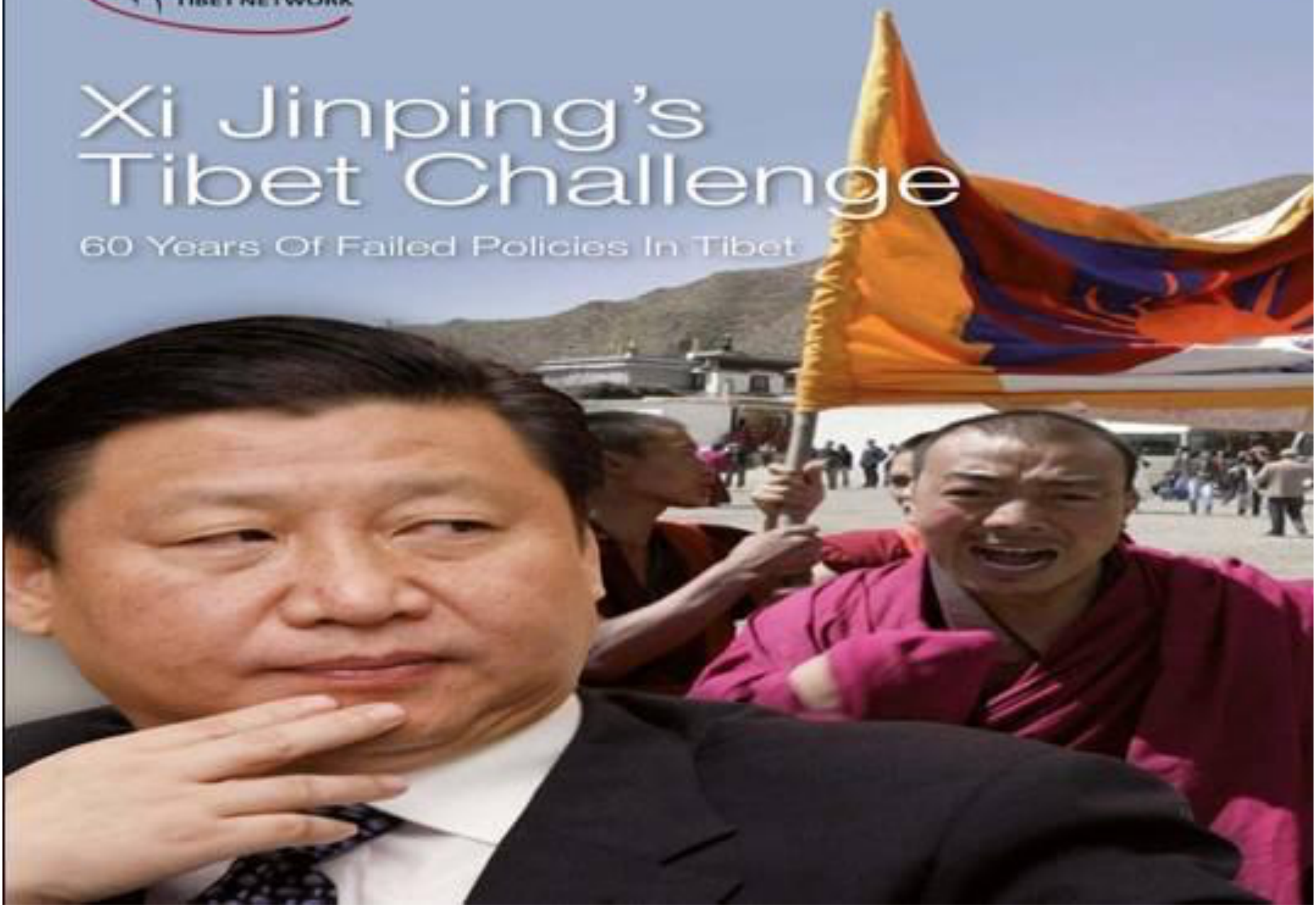
Thanks.

Tibet Network,
1310 Fillmore Street,
Suite 401,San Francisco,
CA 94115 United States
Phone:+91 988 225 5516

INTERNATIONAL TIBET NETWORK

Xi Jinping's Tibet Challenge

60 Years Of Failed Policies In Tibet



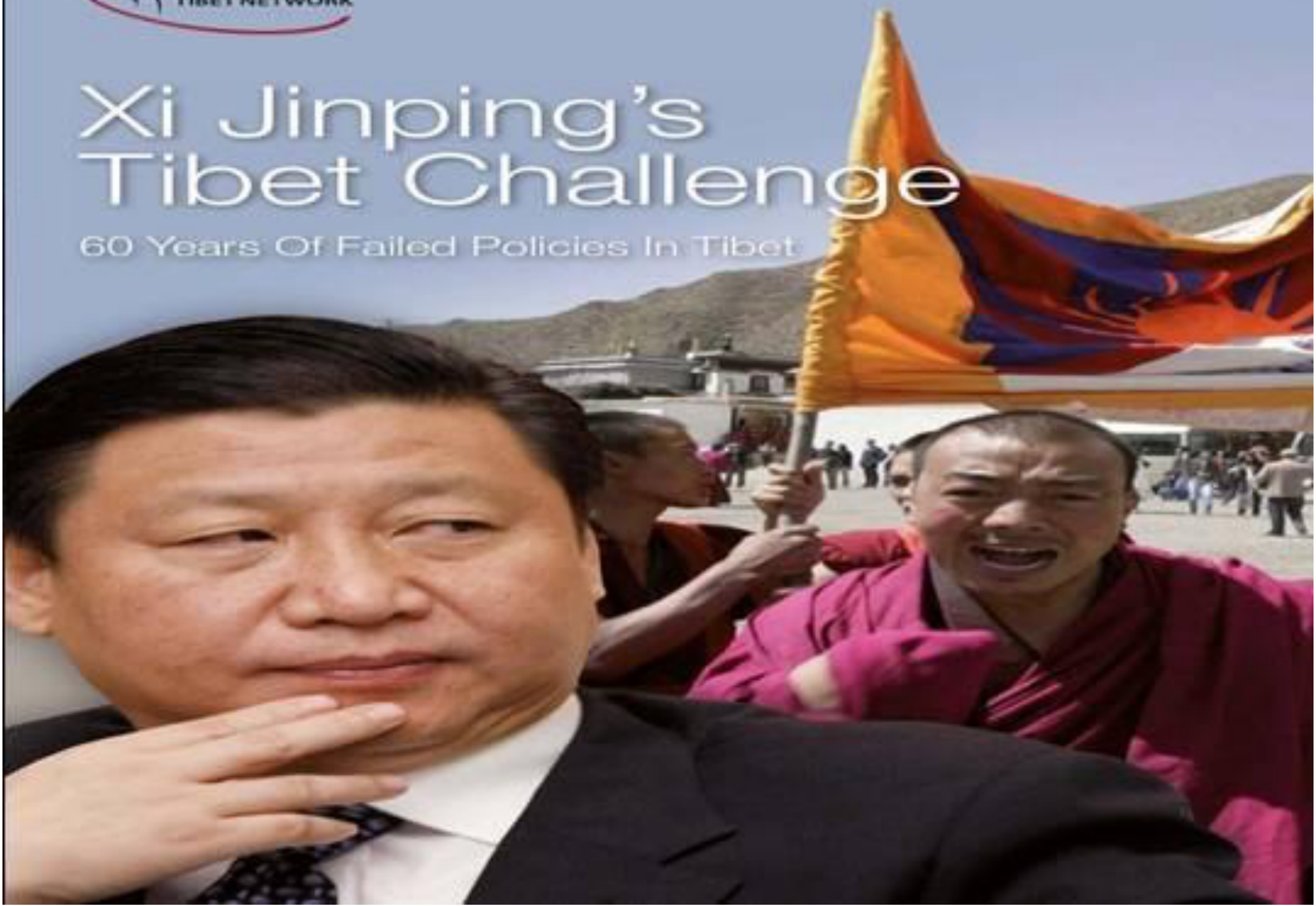
“Sandworm”

- Vulnerabilities in OLE package manager
  - CVE 2014 4114, CVE 2014 6352
  - Original: load remote .inf and “.gif” file
  - Later: from temp folder, no need to worry about firewalls, etc
- Vector: .pps / .ppsx
  - Launches slide deck automatically
- Logic error: no crash or obvious signs to user that they had been compromised

INTERNATIONAL TIBET NETWORK

Xi Jinping's Tibet Challenge

60 Years Of Failed Policies In Tibet



རྒྱུད་སྡོམ་དང་ཁ་བྲལ།

རྒྱུད་སྡོམ་ལས་ལོག་གས་སུ་ཐོན་པའི་ལམ་ཁ་དག་གཤམ་གསལ།

1 ཁེད་ཀྱི་ཡིག་ཆམ་ནང་འབྱོར་བའི་རྒྱུད་སྡོམ་རིགས། པབ་ལེན་དང་ཁ་འབེད་གཉིས་ཀ་མ་བྱེད།

2 བློག་འཕྲིན་ཀྱི་བརྡོད་བྱ་ལ་གཙང་བ་ཤུས་ SCAN ཟེར་ནས་བྱིས་ཤིང་། རྒྱུད་སྡོམ་དེ་ scan@virustotal.com ལ་བཏང་ནས་ད་འབུ་ཡོད་མེད་བརྟག་དཔྱད་བྱོས།

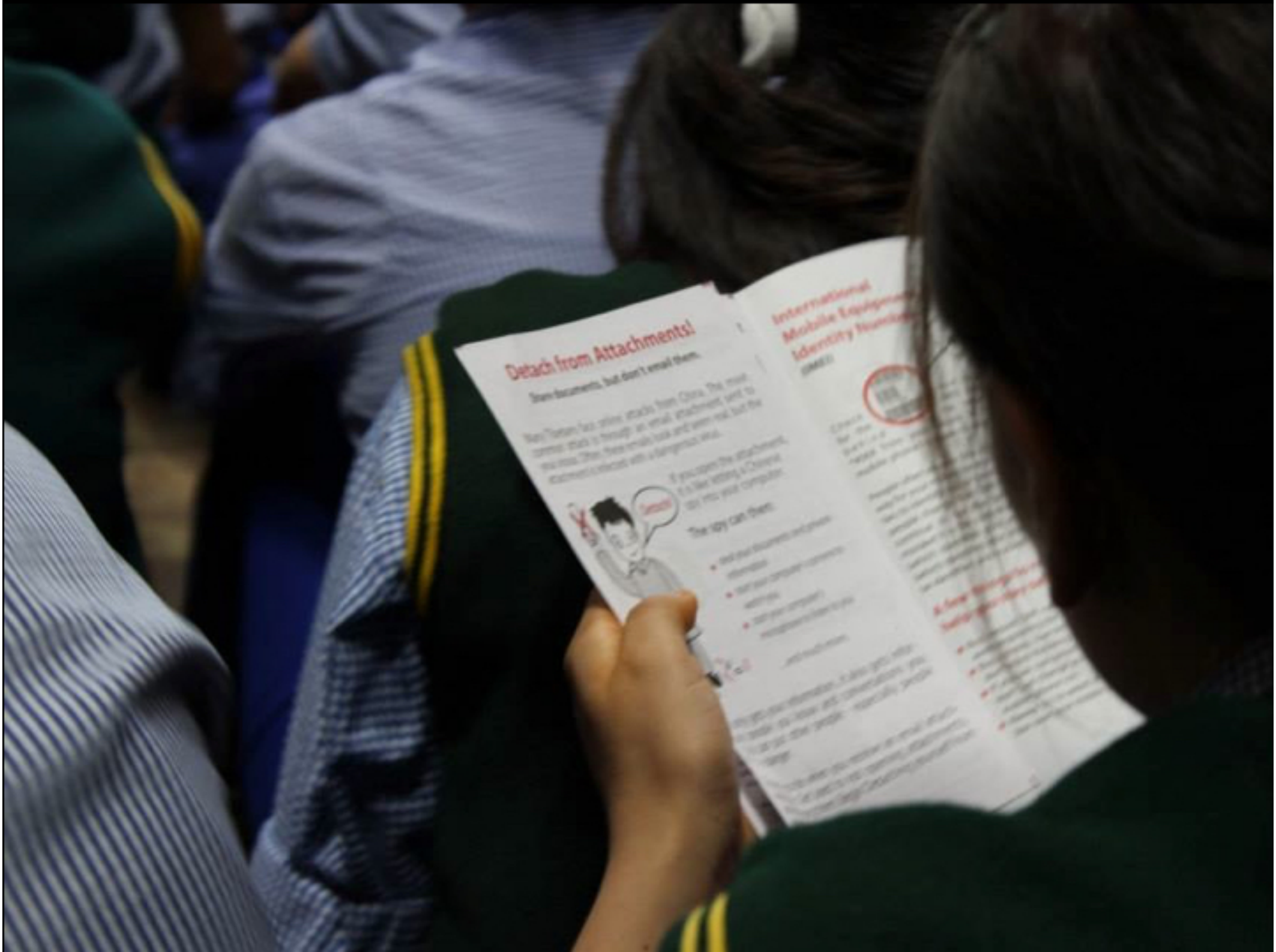
3 རྒྱུད་སྡོམ་དེ་ཁེད་ཀྱི་བློག་ཏུད་སྐང་ལ་ཐད་ཀར་པབ་ ལེན་མ་བྱས་པར། སྒོ་ཌུ་ཆལ་ Google ཀྱི་སྟོན་བཟླ་ "Preview"བརྒྱུད་ནས་རྒྱུད་སྡོམ་དེར་ལྟོས།

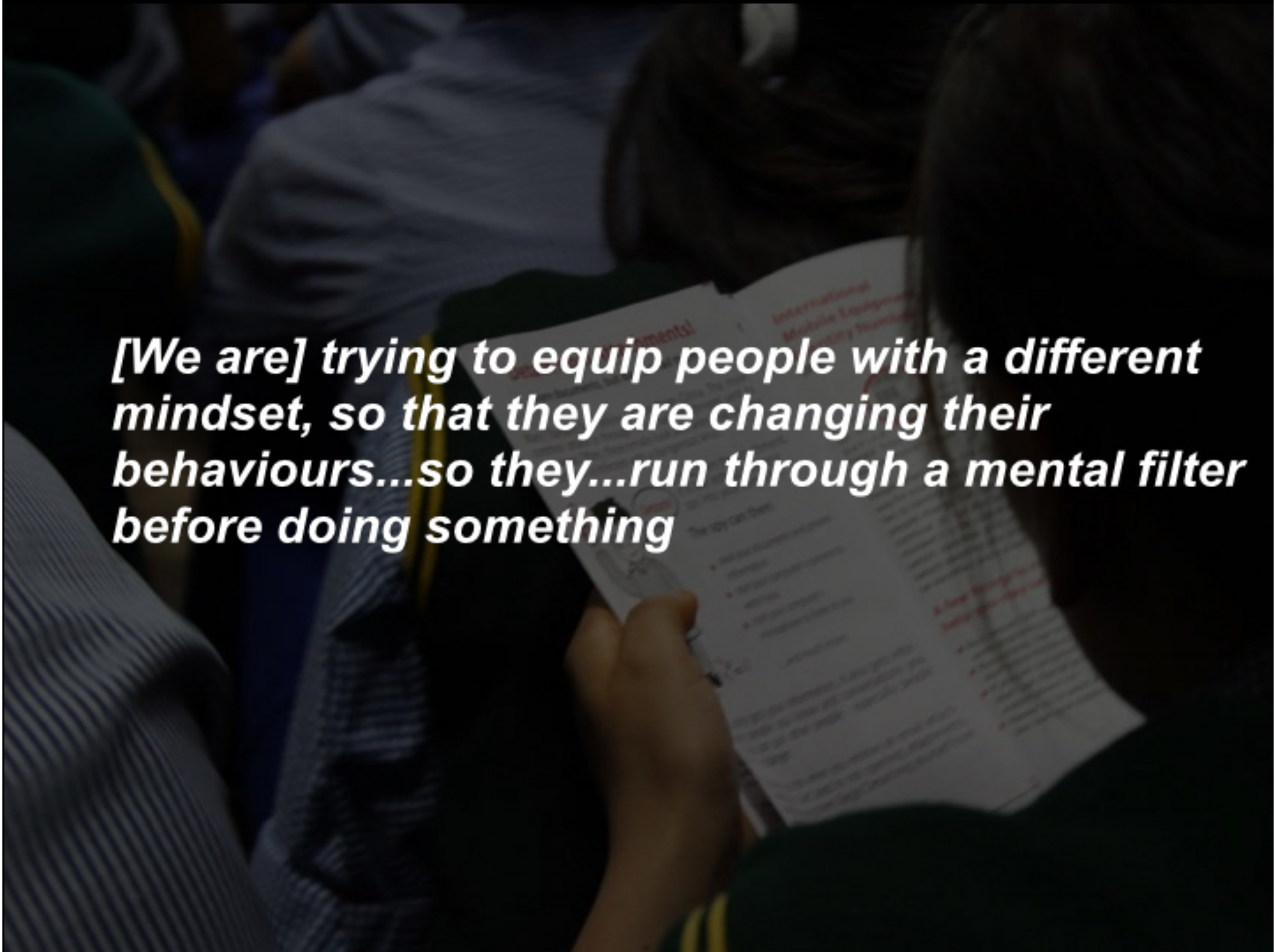
4 རྒྱུད་སྡོམ་དེ་ཁེད་ཀྱི་བློག་པོ་དང་ལས་རོགས་ཚོར་མ་གཏོང་། ཁོང་ཚོར་ཡང་ཁེད་ལ་རྒྱུད་སྡོམ་མ་གཏོང་ཞེས་དེ་སྐུལ་བྱོས།

5 ཡིག་ཆ་དག་བགོ་འཕྲེམས་བྱེད་པར། མི་རྣམས་ལ། GoogleDocs དང་ Dropbox དུ་དུད། www.ge.tt བཅས་སེང་སྟོང་གཏོང་རྒྱུར་མེམས་ཤུགས་སྤར།

Google docs Dropbox GE.TT

Tibet Action Institute
བོད་ཀྱི་ལས་ཀའུ་པའི་གཞུང་ཚང་
http://tibetaction.net


Detach from Attachments!
International Mobile Equipment Identity


[We are] trying to equip people with a different mindset, so that they are changing their behaviours...so they...run through a mental filter before doing something

From Tibet News <tibetnews2015@gmail.com <mailto:tibetnews2015@gmail.com>>

Subject **Biography of H.H. THE 14TH DALAI LAMA**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete

2015-05-06 05:12 AM

Dear Sir/Madam,

I have shared the Biography of H.H. THE 14TH DALAI LAMA via Google Drive.

Kindly download it.

H.H. THE 14TH DALAI LAMA.pps <hxxps://docs.google.com/file/d/0B7vlM3esIIq-YUdFZXYxUUl1Qlk/edit?usp=drive_web>

With Warm Regard,

Tibet News Group
Contact Address: 1228, 17th Street NW, New Delhi
E-mail: tibetnews2015@gmail.com <mailto:tibetnews2015@gmail.com>


“[Technology is] this funny thing where it’s a life line, and then it’s...maybe your ticket to jail”
- Tibetan Activist

“Threat Actors”

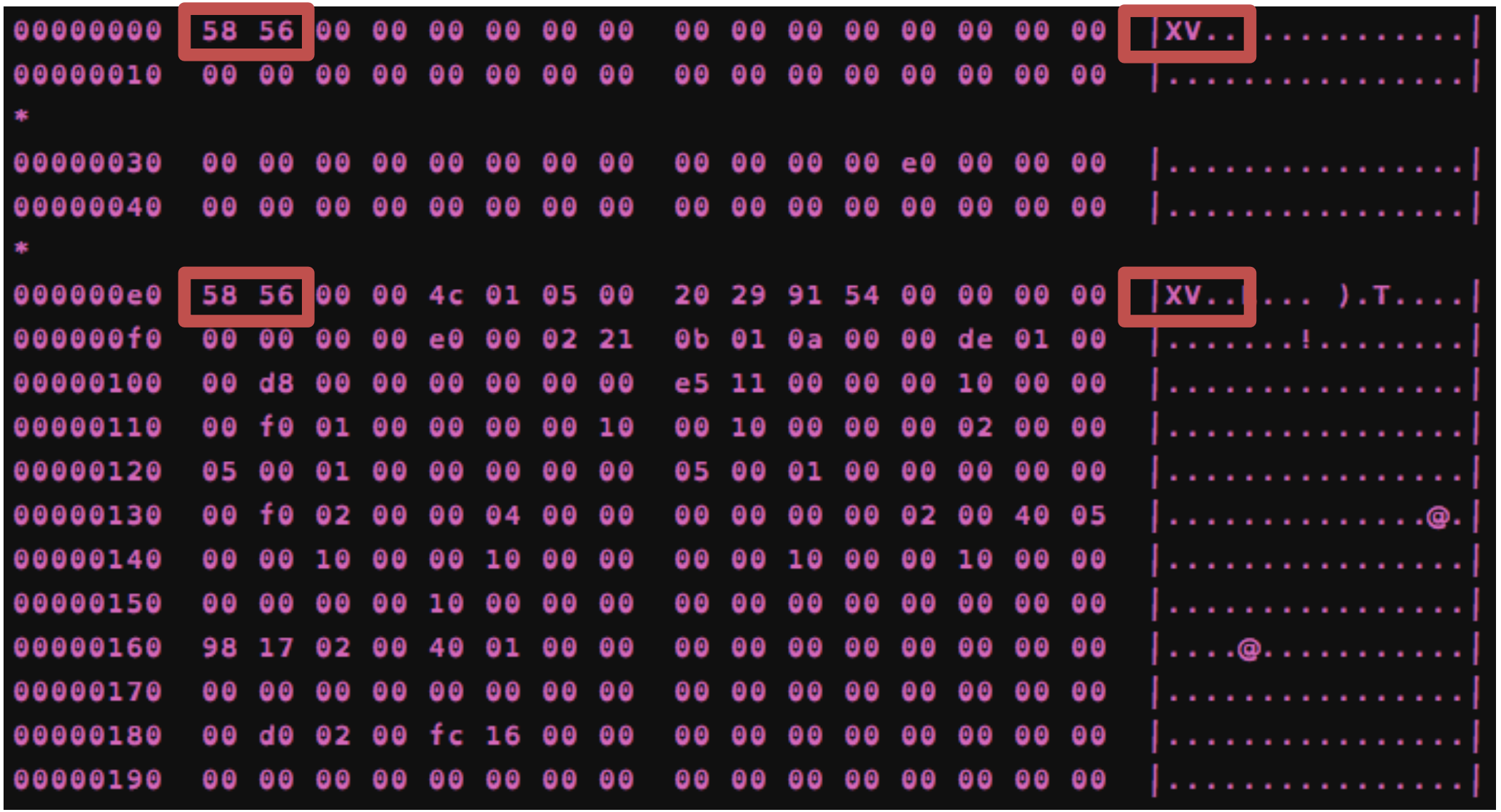
- How to identify connections between different campaigns?
  - Malware families
    - Source code may be publicly available, RAT may be sold
      - Typically in Asia, we see “home grown” RATs vs repurposed crimeware (Syria), or commercial malware (FinFisher/Hacking Team)
  - Command and control infrastructure
  - Contextual information

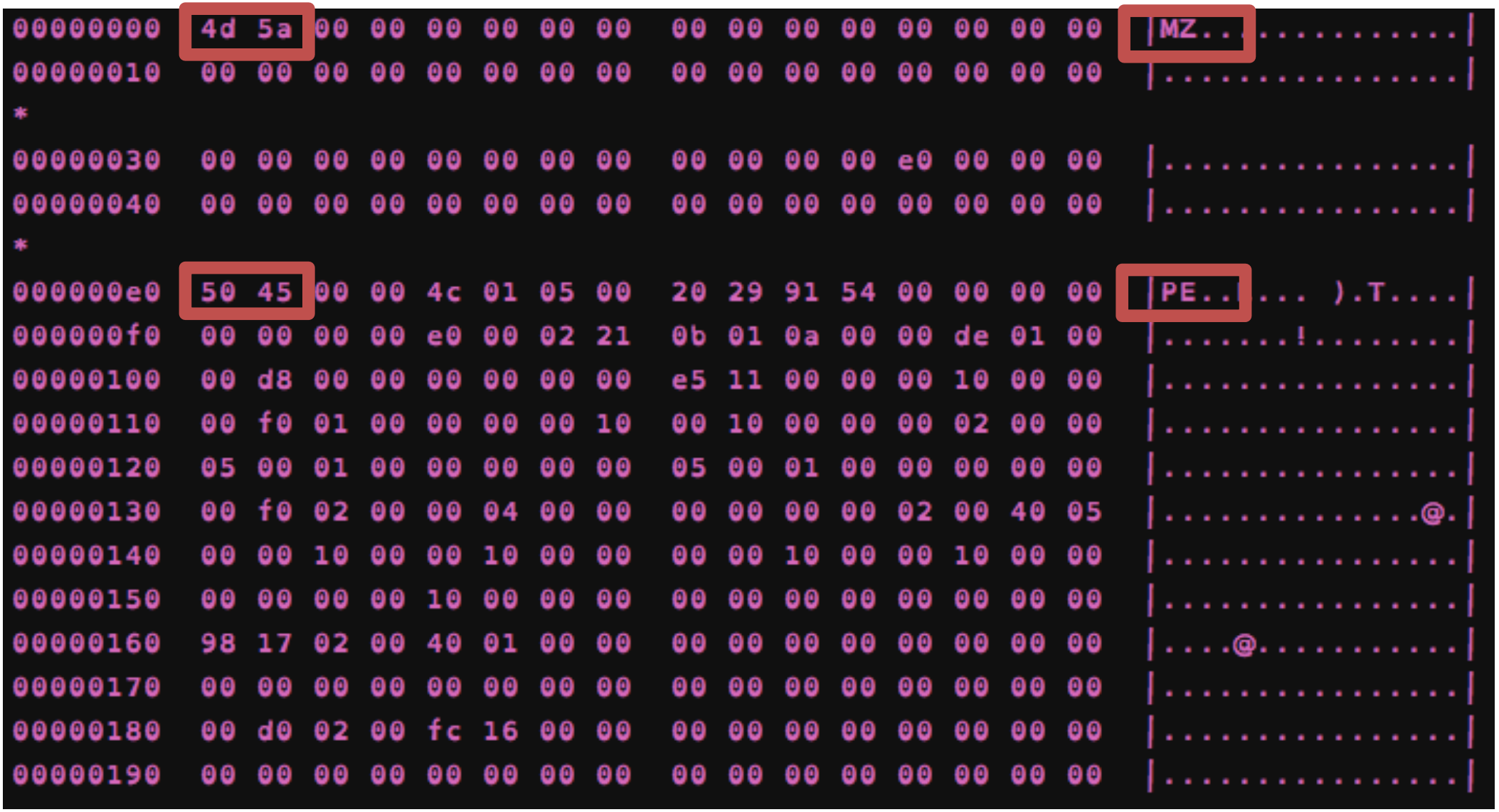
PlugX

- Been under active use /development since at least 2012
  - Originally contained debug messages, pdb paths and “THIS IS A DEMO VERSION!”
  - AlienVault report identified the creator based on evidence like the pdb path
    - Disappeared for a bit after the report
    - Resurfaced with the identified indicators scrubbed

PlugX

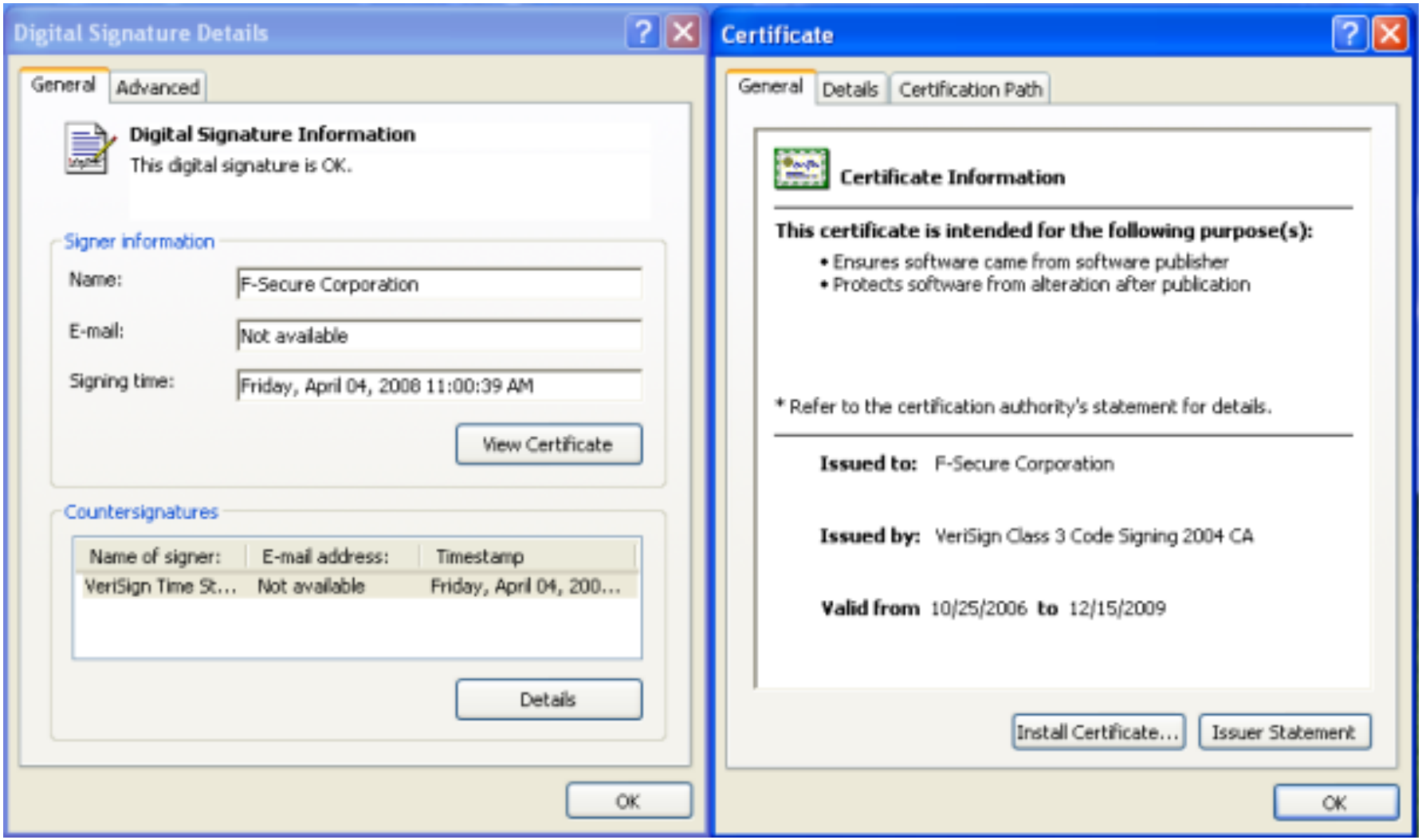
- Uses DLL side loading (WinSxS vs KnownDLLs)
  - Signed legitimate executable
    - So a signed executable is running and added as a service
  - Malicious DLL
  - Encrypted binary containing payload
    - Payload is only ever decrypted in memory to hinder detection and analysis


00000000 58 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |XV..............|
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
*
00000030 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 |................|
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
*
000000e0 58 56 00 00 4c 01 05 00 20 29 91 54 00 00 00 00 |XV..L...).T....|
000000f0 00 00 00 00 e0 00 02 21 0b 01 0a 00 00 de 01 00 |.......!........|
00000100 00 d8 00 00 00 00 00 00 e5 11 00 00 00 10 00 00 |................|
00000110 00 f0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 |................|
00000120 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 |................|
00000130 00 f0 02 00 00 04 00 00 00 00 00 00 02 00 40 05 |..............@.|
00000140 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 |................|
00000150 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |................|
00000160 98 17 02 00 40 01 00 00 00 00 00 00 00 00 00 00 |....@...........|
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
00000180 00 d0 02 00 fc 16 00 00 00 00 00 00 00 00 00 00 |................|
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|


00000000 4d 5a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |MZ..............|
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
*
00000030 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 |................|
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
*
000000e0 50 45 00 00 4c 01 05 00 20 29 91 54 00 00 00 00 |PE..L...).T....|
000000f0 00 00 00 00 e0 00 02 21 0b 01 0a 00 00 de 01 00 |........!........|
00000100 00 d8 00 00 00 00 00 00 e5 11 00 00 00 10 00 00 |................|
00000110 00 f0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 |................|
00000120 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 |................|
00000130 00 f0 02 00 00 04 00 00 00 00 00 00 02 00 40 05 |..............@.|
00000140 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 |................|
00000150 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |................|
00000160 98 17 02 00 40 01 00 00 00 00 00 00 00 00 00 00 |....@...........|
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
00000180 00 d0 02 00 fc 16 00 00 00 00 00 00 00 00 00 00 |................|
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|

- Typical features: key logger, screenshots, enumerating files, etc
- Configure multiple C2s
- Use alternate DNS to avoid detection through organization's logs
- Multiple communications protocols: TCP, UDP, P2P

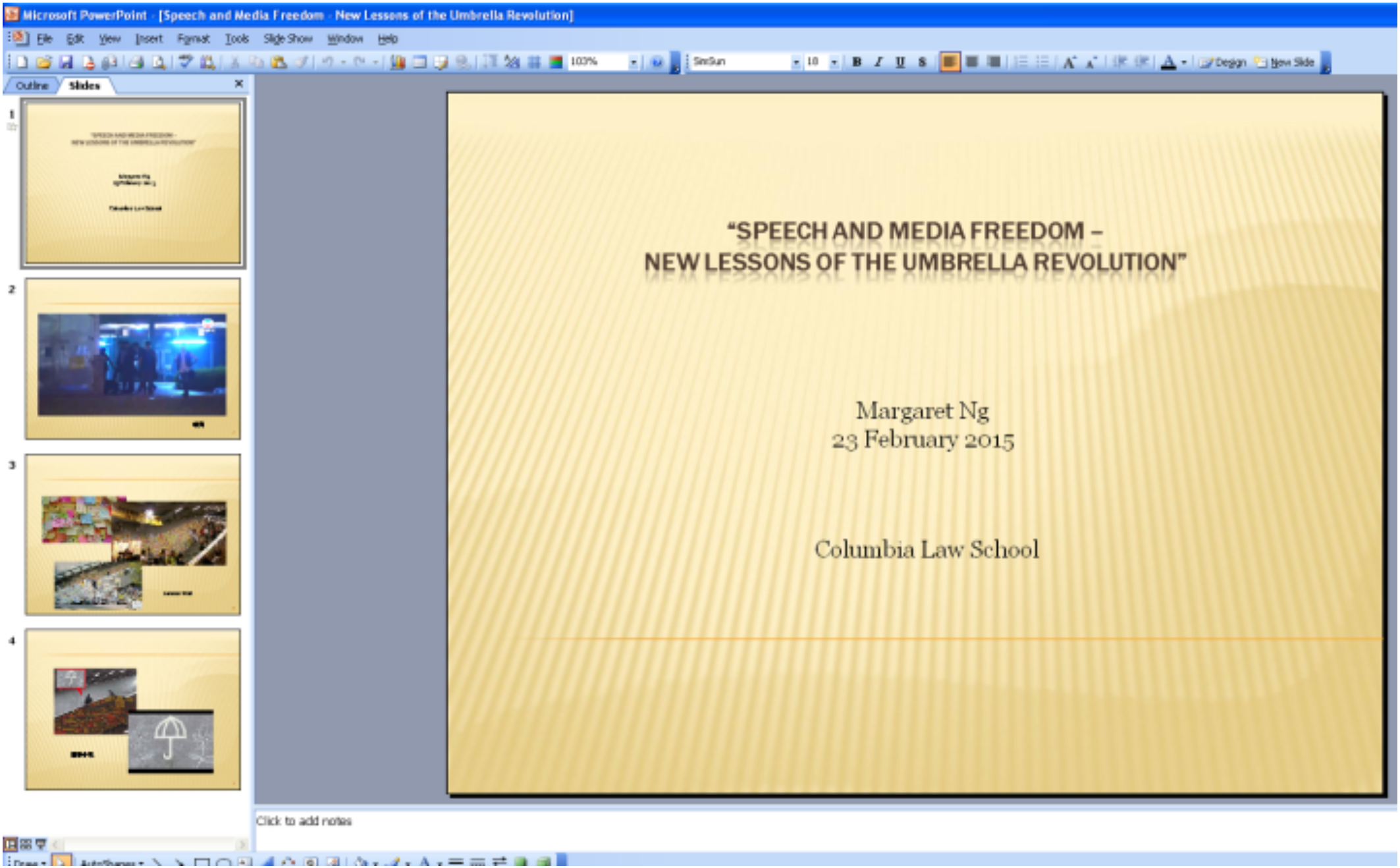
Favorite target for side loading?
AV Vendors!




Hong Kong

Hong Kong

- Spring 2015: Same PlugX malware embedded into two different malicious PowerPoint slideshows
  - One sent to a Tibetan group (shown earlier) repurposing slides from an ITN presentation
  - Another sent to individuals related to pro-democratic political parties featuring Occupy Central related lure


Microsoft PowerPoint - [Speech and Media Freedom - New Lessons of the Umbrella Revolution]
File Edit View Insert Format Tools Slide Show Window Help
Outline
Slides
"SPEECH AND MEDIA FREEDOM –
NEW LESSONS OF THE UMBRELLA REVOLUTION"
Margaret Ng
23 February 2015
Columbia Law School
Click to add notes

Extent of overlap?

- The same threat actor?
- Commonalities across attacks indicate at least *some* form of resource sharing between attackers
- Our focus is NGOs but we've seen overlap with well documented attacks against industry and government
  - –Mandiant's APT1, and others

"Sule-Pagoda by-Night". Licensed under Attribution via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Sule-Pagoda_by-Night.jpg#/media/File:Sule-Pagoda_by-Night.jpg

Political and Economic Context

- Burma is undergoing political and economic transformation
- Country is rich in natural resources (e.g, oil, gas, minerals, timber, etc)
- Heavy investment from China in commercial development
- NGOs are concerned over environmental and human rights impact of development

From redacted

Subject **Japanese firms apply to operate in SEZs Permit.**

To [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete

2015-06-05 02:15 PM

Dear all,

Japanese firms apply to operate in SEZs Permit.

Permit.zip
<hxxps://drive.google.com/file/d/0B-FCGIKuUvEQX3Y4RmlyaDI4N00/edit?usp=drive_web>

Japanese firms apply to operate in SEZs

Among the international insurance firms that have representative offices in Myanmar, only Japanese firms have applied to operate in special economic zones, according to the supervisory board of Myanma Insurance.

Sixteen foreign insurance firms have opened representative offices in Myanmar, but they have not begun operations since regulations have not yet been fully disclosed.

“We will give them permits to begin operating as soon after the principles are issued,” said Dr Maung Maung Thein, the chairperson of the supervisory board.

Only those who meet the criteria will be given the green light. The insurance firms will first be permitted to operate in Myanmar’s three SEZs: Thilawa, Kyaukphyu and Dawei.

From: [redacted]
Subject: **Japanese firms apply to operate in SEZs Permit.**
To: [redacted]

Reply | Reply All | Forward | Archive | Junk | Delete

2015-06-05 02:15 PM

Dear all,

Japanese firms apply to operate in SEZs Permit.

Permit.zip
<hxxps://drive.google.com/file/d/0B-FCGIKuUvEQX3Y4RmlyaDI4N00/edit?usp=drive_web>

- Permit/Permit.jpg.lnk (In archive)
  - ca-bundle.exe (Downloaded)
    - AwViewWx.exe (Downloaded)
      - mcf.ep (Embedded)
      - mcf.exe (Embedded)
      - mcutil.dll (Embedded)

From redacted

Subject Japanese firms apply to operate in SEZs Permit.

To

Reply | Reply All | Forward | Archive | Junk | Delete

2015-06-05 02:15 PM

Dear all,

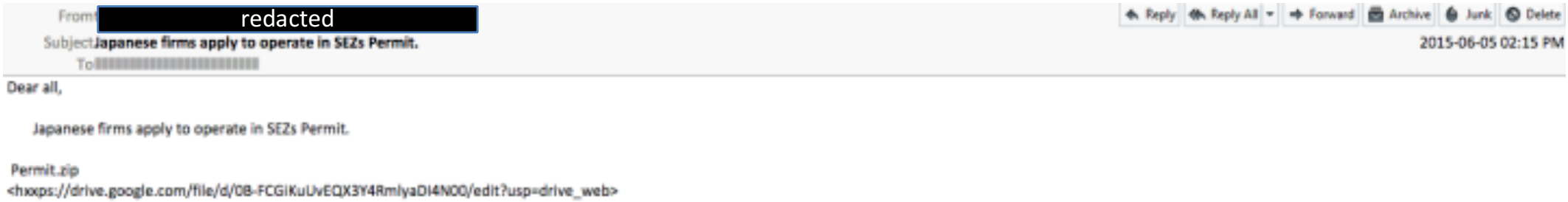
Japanese firms apply to operate in SEZs Permit.

Permit.zip
<hxxps://drive.google.com/file/d/0B-FCGIKuUvEQX3Y4RmlyaDI4N00/edit?usp=drive_web>

- Permit/Permit.jpg.lnk (In archive)
  - ca-bundle.exe (Downloaded)
    - AwViewWx.exe (Downloaded)
      - mcf.ep (Embedded)
      - mcf.exe (Embedded)
      - mcutil.dll (Embedded)

PlugX!

Surprise!



- Permit/Permit.jpg.lnk (In archive)
  - ca-bundle.exe (Downloaded)
    - AwViewWx.exe (Downloaded)
      - mcf.ep (Embedded)
      - mcf.exe (Embedded)
      - mcutil.dll (Embedded)

PlugX!

Surprise!

From: [redacted]
Subject: **Japanese firms apply to operate in SEZs Permit.**
To:

Reply | Reply All | Forward | Archive | Junk | Delete

2015-06-05 02:15 PM

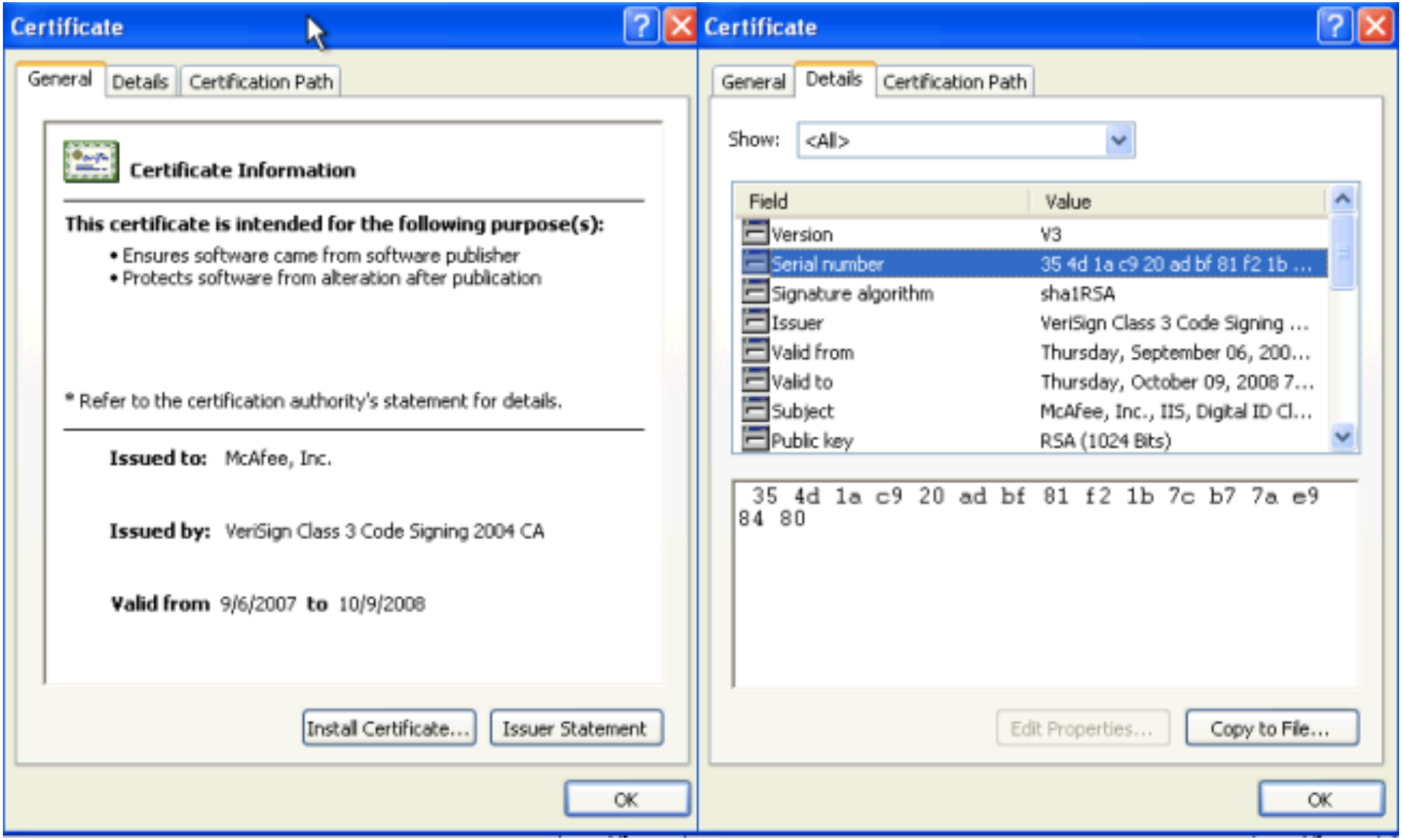
Dear all,

Japanese firms apply to operate in SEZs Permit.

Permit.zip
<hxxps://drive.google.com/file/d/0B-FCGIKuUvEQX3Y4RmlyaDI4N00/edit?usp=drive_web>

- Permit/Permit.jpg.lnk (In archive)
  - ca-bundle.exe (Downloaded)
    - AwViewWx.exe (Downloaded)
      - mcf.ep (Embedded)
      - mcf.exe (Embedded)
      - mcutil.dll (Embedded)

PlugX!


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures software came from software publisher
• Protects software from alteration after publication
* Refer to the certification authority's statement for details.
Issued to: McAfee, Inc.
Issued by: VeriSign Class 3 Code Signing 2004 CA
Valid from 9/6/2007 to 10/9/2008
Install Certificate...
Issuer Statement
OK
Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Version
V3
Serial number
35 4d 1a c9 20 ad bf 81 f2 1b ...
Signature algorithm
sha1RSA
Issuer
VeriSign Class 3 Code Signing ...
Valid from
Thursday, September 06, 200...
Valid to
Thursday, October 09, 2008 7...
Subject
McAfee, Inc., IIS, Digital ID Cl...
Public key
RSA (1024 Bits)
35 4d 1a c9 20 ad bf 81 f2 1b 7c b7 7a e9
84 80
Edit Properties...
Copy to File...
OK

Connections with other campaigns?

- Malware using related C2 signed using same revoked certificate as in attacks against Tibetan organizations
  - PlugX, EvilGrab
- Large volume of attacks in Burma around the same time using the same malware families

uh oh...

“oh dear lord everyone is owned”

14 Jan — နိုင်ငံတော်သမ္မတ ဦးသိန်းစိန် အပြည်ပြည်ဆိုင်ရာ ကြက်ခြေနီကော်မတီ ဥက္ကဋ္ဌအား လက်ခံတွေ့ဆုံ

11 Jan — နိုင်ငံတော်သမ္မတ အဆေးစားနှင့်အလတ်စား စီးပွားရေးလုပ်ငန်းများ အစည်းအဝေးသို့ တက်ရောက်

11 Jan — နိုင်ငံတော်သမ္မတဦးသိန်းစိန် ဟန်ဂေရီနိုင်ငံ လွှတ်တော်ရေးရာ ဝန်ကြီးအား လက်ခံတွေ့ဆုံ

10 Jan — နိုင်ငံတော်သမ္မတက ပြည်ထောင်စုလွှတ်တော်သို့ နှစ်သစ်ကူးသဝဏ်လွှာ ပေးပို့ခြင်း

နောက်ဆုံးရသတင်းများ

တိုင်းရင်းဆေးကောင်စီဥပဒေကို ပြင်ဆင်သည့် ဥပဒေ

တိုင်းရင်းဆေးကောင်စီဥပဒေကို ပြင်ဆင်သည့် ဥပဒေ

တိုက်ရိုက်ထုတ်လွှင့်မှု

Auto start on | off

EVILGRAB DELIVERED BY WATERING HOLE ATTACK ON PRESIDENT OF MYANMAR'S WEBSITE

POSTED BY: Robert Falcone on June 11, 2015 7:00 PM

FILED IN: Malware, Unit 42
TAGGED: Evilgrab, IFRAME, JavaScript, Myanmar, Trojan, Vidgrab, Watering Hole Attack

On May 12, 2015, Unit 42 observed an apparent watering hole attack, also known as a strategic website compromise (SWC), involving the President of Myanmar's website. Visiting the main page hosted at "www.president-office.gov[.]mm" triggered the malicious content, as the threat actors injected an inline frame (IFRAME) into a JavaScript file used by Drupal for the site's theme.

Unit 42 believes threat actors chose this website to set up a watering hole in order to target and gather information on individuals in Myanmar, individuals involved in political relations with the country and/or organizations doing business in Myanmar. Unit 42 has evidence to suggest the threat actors have had access to the website since November 2014 if not earlier.

Attack identified after "globally recognized organization in the oil and gas industry" visited the URL containing the malicious code

Index of /mmpdd/sites/default/files/field

Name	Last modified	Size	Description
Parent Directory		-	
IBMAPP.exe	08-Jul-2015 01:29	32K	
fibmapp.exe	15-Jul-2015 23:33	241K	
fields.exe	07-Jul-2015 23:50	320K	
image/	06-Feb-2013 09:31	-	

Apache/2.2.15 (CentOS) Server at www.moi.gov.mm Port 80

image source: https://asert.arbornetworks.com/defending-the-white-elephant/

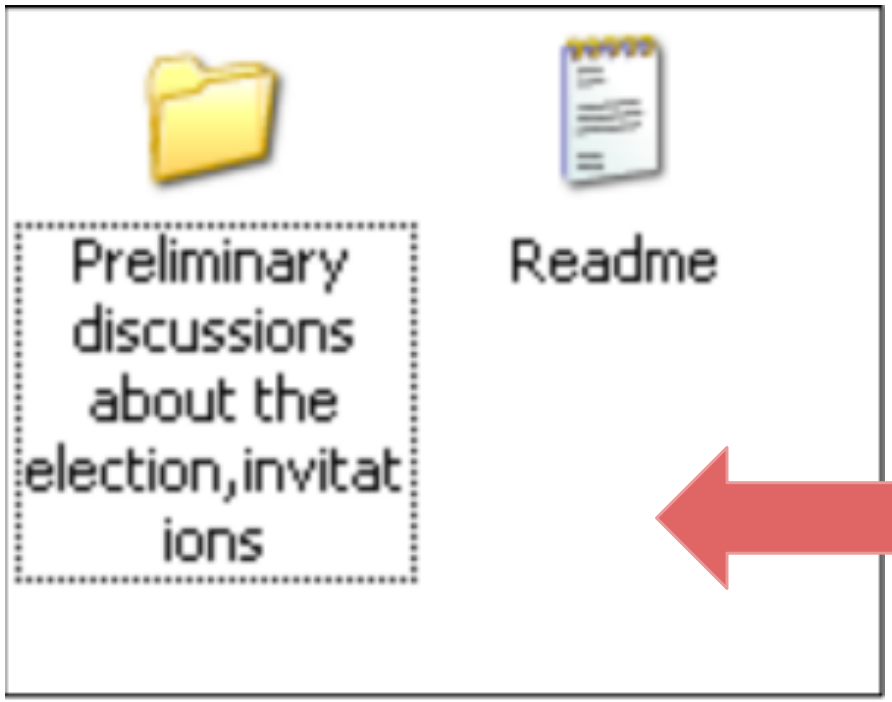


image source:
https://asert.arbornetworks.com/defending-the-white-elephant/

PlugX

Same McAfee executable!

From: **office** <hinthin1asd23@gmail.com>
Date: Sun, Aug 16, 2015 at 7:47 PM
Subject: Burma Gags Media Linked to Shwe Mann, Adding to Concerns About Reforms
To [redacted]

Burma Gags Media Linked to Shwe Mann, Adding to...

THE IRRAWADDY
COVERING BURMA AND SOUTHEAST ASIA

PARTY POLITICS

Burma Gags Media Linked to Shwe Mann, Adding to Concerns About Reforms

Related Readings

- Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites https://citizenlab.org/2015/10/targeted-attacks-ngo-burma
- Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114 https://citizenlab.org/2015/06/targeted-attacks-against-tibetan-and-hong-kong-groups-exploiting-cve-2014-4114/
- Communities @ Risk https://targetedthreats.net
- Indicators: https://github.com/citizenlab/malware-indicators

Targeted Attacks Deep Analysis: Case Study in Hong Kong

VXRL

HITB GSEC Singapore 2015

Disclaimer

*** No national secrets ^_^: ***

Case Study about APT against Hong Kong

- Observation
- Against people in the political movement
- Against Voting Website

Observation

We analysed around 40 samples and incidents from the past 18 months against NGOs/Democrats/University sites and obtain the following observation

Who are they?

We never know as I just know they know Chinese characters and didn’t capture any last mile of traffic, we are not talented as mandiant, could guess which dept from a particular string like this: 1j2b3c (Please refer to APT1 report) :)

Where are they?

Most of them put their C2 and VPS in Hong Kong in 2nd/3rd of Internet Service Providers.

Observation

Their favorite payload

They do like RATs always: JRAT, PoisonIvy, ….etc, but as I said I can't see they use TeamViewer, this link is for "their" reference to consider other RATs :)

http://sniperhaxx.blogspot.hk/2014/09/top-ten-ratremote-administration-tools.html

Single Server Serves Different Purposes

Sometimes, we have found those servers, could be C2, serve different purpose. For example, It could serve a phishing site or malware download and C2 together against a single target. It looks the operator didn't care about the secrecy of command and control server.

Observation Against Democrats/Human Rights/NGOs/Media

There are many ways to attack and we simply classify them into various level based on sophistication and expertise. The percentage stands for the proportion.

Level 0: Web Defacement and Phishing Site (20%)

Level 1: Putting an executable or/and hidden frame and link in the compromised site (10%)

Level 2: Sending phishing mails from Google Gmail/Yahoo Gmail/Dropbox/Whatsapp (20%)

Level 3: Sending malicious attachment with exploits (commonly in MS Office and PDF) with RAT as payload including PoisonIvy and Java RAT as well as VNC (35%)

Observation Against Democrats/Human Rights/NGOs/Media

Level 4: Sending more “advanced” exploitation with “customised” encryption with use of XOR. It is not common in Hong Kong case but Taiwan (5%)

Level 5: Make a malicious mobile application or software for espionage purpose. (5%)

Level 6: DDoS attack against a site for important political events (5%)

In coming 10 minutes

We will illustrate attacks in levels 5 and 6 so that you could get to know more about the techniques and their revolution as well as their “commitment” :-)

All attacks are happened during Occupying Central, called Umbrella Movement, in Hong Kong.

Case Study #1: Fake Mobile Application

It spoofs CodeForHK organisation to send out a SMS message to people who could download an application to coordinate OccupyCentral movement

Credit and appreciation to CodeForHK fellows and Matthew for this analysis, it is good to work with them for the analysis.

Story begins

1. Hacking QQ

When it boots it copies assets/qq xml to the locatio "/sdcard/.qq/temp apk". it attempts to hijack victim's application.

```
104     :try_start_0
105     invoke-virtual {p0}, Lcom/v1/MainActivity;->getAssets()Landroid/content/res/AssetManager;
106
107     move-result-object v0
108
109     const-string v1, "qq.xml"
110
111     invoke-virtual {v0, v1}, Landroid/content/res/AssetManager;->open(Ljava/lang/String;)Ljava/io/InputStream;
112
113     move-result-object v0
114
115     new-instance v1, Ljava/io/File;
116
117     const-string v2, "/sdcard/.qq/"
118
119     invoke-direct {v1, v2}, Ljava/io/File;-><init>(Ljava/lang/String;)V
120
121     invoke-virtual {v1}, Ljava/io/File;->mkdir()Z
122
123     new-instance v1, Ljava/io/FileOutputStream;
124
125     const-string v2, "/sdcard/.qq/temp.apk"
126
127     invoke-direct {v1, v2}, Ljava/io/FileOutputStream;-><init>(Ljava/lang/String;)V
128
129     const/16 v2, 0x400
130
131     new-array v2, v2, [B
132
```

2. Capture Outgoing Call

It hooks into any outgoing calls

```
<receiver android:name="com.v1.PhoneReceiver" android:priority="2147483647">
    <intent-filter>
        <action android:name="android.intent.action.PHONE_STATE"/>
        <action android:name="android.intent.action.NEW_OUTGOING_CALL"/>
    </intent-filter>
</receiver>
```

And seems to record them

And stores them at "`/data/data/com.v1/XXXXXX.amr`"

```
452
453     invoke-virtual {v0}, Landroid/media/MediaRecorder;->release()V
454
455     sput-object v6, Lcom/v1/PhoneReceiver;->d:Landroid/media/MediaRecorder;
456
457     sput-boolean v5, Lcom/v1/StreamService;->e:Z
458
459     :cond_5
460     sget-boolean v0, Lcom/v1/StreamService;->e:Z
461
462     if-nez v0, :cond_2
463
464     new-instance v0, Landroid/media/MediaRecorder;
465
466     invoke-direct {v0}, Landroid/media/MediaRecorder;-><init>()V
467
468     sput-object v0, Lcom/v1/PhoneReceiver;->d:Landroid/media/MediaRecorder;
469
470     invoke-virtual {v0, v2}, Landroid/media/MediaRecorder;->setAudioSource(I)V
471
472     sget-object v0, Lcom/v1/PhoneReceiver;->d:Landroid/media/MediaRecorder;
473
474     invoke-virtual {v0, v2}, Landroid/media/MediaRecorder;->setOutputFormat(I)V
475
476     sget-object v0, Lcom/v1/PhoneReceiver;->d:Landroid/media/MediaRecorder;
477
478     invoke-virtual {v0, v2}, Landroid/media/MediaRecorder;->setAudioEncoder(I)V
479
480     new-instance v0, Ljava/lang/StringBuilder;
481
482     const-string v1, "in_"
483
484     invoke-direct {v0, v1}, Ljava/lang/StringBuilder;-><init>(Ljava/lang/String;)V
485
486     sget-object v1, Lcom/v1/PhoneReceiver;->c:Ljava/lang/String;
487
488     invoke-virtual {v0, v1}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
```

```
519
520     invoke-virtual {v0}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
521
522     move-result-object v0
523
524     new-instance v1, Ljava/io/File;
525
526     const-string v2, "/data/data/com.v1/.record/"
527
528     invoke-direct {v1, v2}, Ljava/io/File;-><init>(Ljava/lang/String;)V
529
530     invoke-virtual {v1}, Ljava/io/File;->mkdirs()Z
531
532     sget-object v1, Lcom/v1/PhoneReceiver;->d:Landroid/media/MediaRecorder;
533
534     new-instance v2, Ljava/lang/StringBuilder;
535
536     const-string v3, "/data/data/com.v1/.record/"
537
538     invoke-direct {v2, v3}, Ljava/lang/StringBuilder;-><init>(Ljava/lang/String;)V
539
540     invoke-virtual {v2, v0}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
541
542     move-result-object v0
543
544     const-string v2, ".amr"
545
546     invoke-virtual {v0, v2}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;
547
548     move-result-object v0
549
550     invoke-virtual {v0}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
551
```

3. Using Baidu as Geolocation

```
626
627     invoke-virtual {v2, v3}, Lcom/v1/lib/Location;->b(Ljava/lang/String;)V
628
629     const/16 v3, 0xe7
630
631     invoke-virtual {v2, v3}, Lcom/v1/lib/Location;->a(S)V
632
633     move-object/from16 v0, p0
634
635     iget-object v2, v0, Lcom/v1/StreamService;->m:Lcom/baidu/location/LocationClient;
636
637     invoke-virtual {v2}, Lcom/baidu/location/LocationClient;->start()V
638
639     :cond_3
640     :goto_0
641     move-object/from16 v0, p0
642
643     iget-boolean v2, v0, Lcom/v1/StreamService;->i:Z
644     :try_end_0
645     .catch Ljava/net/ConnectException; {:try_start_0 .. :try_end_0} :catch_1
646     .catch Ljava/net/UnknownHostException; {:try_start_0 .. :try_end_0} :catch_3
647     .catch Ljava/io/IOException; {:try_start_0 .. :try_end_0} :catch_5
648     .catch Ljava/lang/RuntimeException; {:try_start_0 .. :try_end_0} :catch_8
649     .catch Ljava/lang/Exception; {:try_start_0 .. :try_end_0} :catch_6
650
```

Other Findings

- Virustotal shows this IP address is used as malware service before in Nov 2013
  - URL: https://www.virustotal.com/en/ip-address/61.36.11.75/information/
- 221.226.58.202 is hardcoded in StreamService
- 101.55.121.36 is suspected to be the C2 server
- Both can be accessed by RDP As of 2014-09-17, it's a Windows 2003 server in simplified Chinese
- Look at the com.google.xrat.protocol stuff, it seems to be able to grab call history, contacts db, SMS history and files on the phone


61.36.11.75
登录到 Windows
Microsoft
Windows Server 2003
Enterprise Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
用户名(U):
密码(P):
确定
取消
选项(O) >>

No more?

Resolve	First	Last	Source	Tags
wottj.click	2015-07-26 00:00:00	2015-07-26 00:00:00	virustotal	
exunf.click	2015-07-26 00:00:00	2015-07-26 00:00:00	virustotal	
fangmz.com	2015-07-18 16:57:14	2015-07-19 01:52:31	riskiq	
aggdns.com	2015-07-15 02:16:25	2015-07-15 08:17:04	riskiq	
www.o6ges.cmkdqv0.cn	2015-07-14 14:22:04	2015-07-14 14:22:04	riskiq	
www.dyh.lsgwu61.cn	2015-07-12 05:33:02	2015-07-12 05:33:02	riskiq	
ythdz.com	2015-06-26 12:20:46	2015-06-26 12:20:46	riskiq	
hanguob0008.sjx88.cn	2015-02-26 17:18:00	2015-02-26 17:18:00	mnemonic	
hanguob0007.sjx88.cn	2015-02-26 17:17:47	2015-02-26 17:17:47	mnemonic	
hanguob0012.sjx88.cn	2015-02-26 17:17:40	2015-02-26 17:17:40	mnemonic	
hanguob0007.sjx88.cn	2015-02-26 00:00:00	2015-02-26 00:00:00	virustotal	
hanguob0012.sjx88.cn	2015-02-26 00:00:00	2015-02-26 00:00:00	virustotal	
hanguob0008.sjx88.cn	2015-02-26 00:00:00	2015-02-26 00:00:00	virustotal	
code4hk.vicp.cc	2014-09-17 00:00:00	2014-09-17 07:36:38	virustotal, kaspersky	dynamic

Resolve	First	Last	Source	Tags
evghr.click	2015-07-29 07:13:56	2015-07-29 07:13:56	riskiq	
fucyj.click	2015-07-28 16:15:26	2015-07-29 07:09:46	riskiq	
sywybb.cn	2015-07-29 07:07:42	2015-07-29 07:07:45	riskiq	
qjnkh.click	2015-07-28 17:34:30	2015-07-29 06:57:17	riskiq	
iwfez.click	2015-07-28 17:48:46	2015-07-29 06:48:06	riskiq	
apvff.click	2015-07-29 06:38:34	2015-07-29 06:38:34	riskiq	
jrkwi.cn	2015-07-29 05:35:52	2015-07-29 05:35:52	riskiq	
gzfdq.click	2015-07-29 05:17:27	2015-07-29 05:17:27	riskiq	
jhgkc.cn	2015-07-29 05:17:06	2015-07-29 05:17:06	riskiq	
ruqtb.click	2015-07-28 23:09:56	2015-07-28 23:09:56	riskiq	
ooket.click	2015-07-28 16:49:00	2015-07-28 20:47:29	riskiq	
gowu888.cn	2015-07-28 00:02:06	2015-07-28 00:02:06	riskiq	
www.r6p.cnlxs.click	2015-07-26 11:25:14	2015-07-26 11:25:14	mnemonic	
www.ji2.cnlxs.click	2015-07-26 11:25:13	2015-07-26 11:25:13	mnemonic	
www.8pg.cnlxs.click	2015-07-26 11:25:13	2015-07-26 11:25:13	mnemonic	

Resolve	First	Last	Source	Tags
yfnis.jiankang.baidu.com.gckyy.cn	2015-10-10 15:54:09	2015-10-10 15:54:09	riskiq	
www.ol14o.vk80pi6.cn	2015-10-09 21:14:37	2015-10-09 21:14:37	riskiq	
www.oj4u.vk80pi6.cn	2015-10-09 21:13:42	2015-10-09 21:13:42	riskiq	
www.ohd.vk80pi6.cn	2015-10-09 21:12:51	2015-10-09 21:12:51	riskiq	
kbvvs.baidu.com.ktvof.cn	2015-10-04 09:02:23	2015-10-04 09:02:23	riskiq	
www.fpz9r.ivhmn.click	2015-08-27 00:00:00	2015-08-27 14:33:06	mnemonic, virustotal	
www.r3ljl.ooket.click	2015-08-26 00:00:00	2015-08-26 22:38:10	mnemonic, virustotal, kaspersky	
bgano.cn	2015-07-29 20:42:24	2015-07-29 20:42:24	riskiq	
kqktv.click	2015-07-29 00:28:39	2015-07-29 18:19:58	riskiq	
gckyy.cn	2015-07-29 17:29:17	2015-07-29 17:29:17	riskiq	
kffwg.click	2015-07-29 15:23:23	2015-07-29 15:23:23	riskiq	
ktvof.cn	2015-07-29 15:19:37	2015-07-29 15:19:37	riskiq	
klend.click	2015-07-29 11:03:22	2015-07-29 14:58:44	riskiq	
ivhmn.click	2015-07-29 09:58:36	2015-07-29 09:58:36	riskiq	
sgrgs.click	2015-07-29 07:19:57	2015-07-29 07:19:57	riskiq	

t c m b

add tag...

101.55.121.36

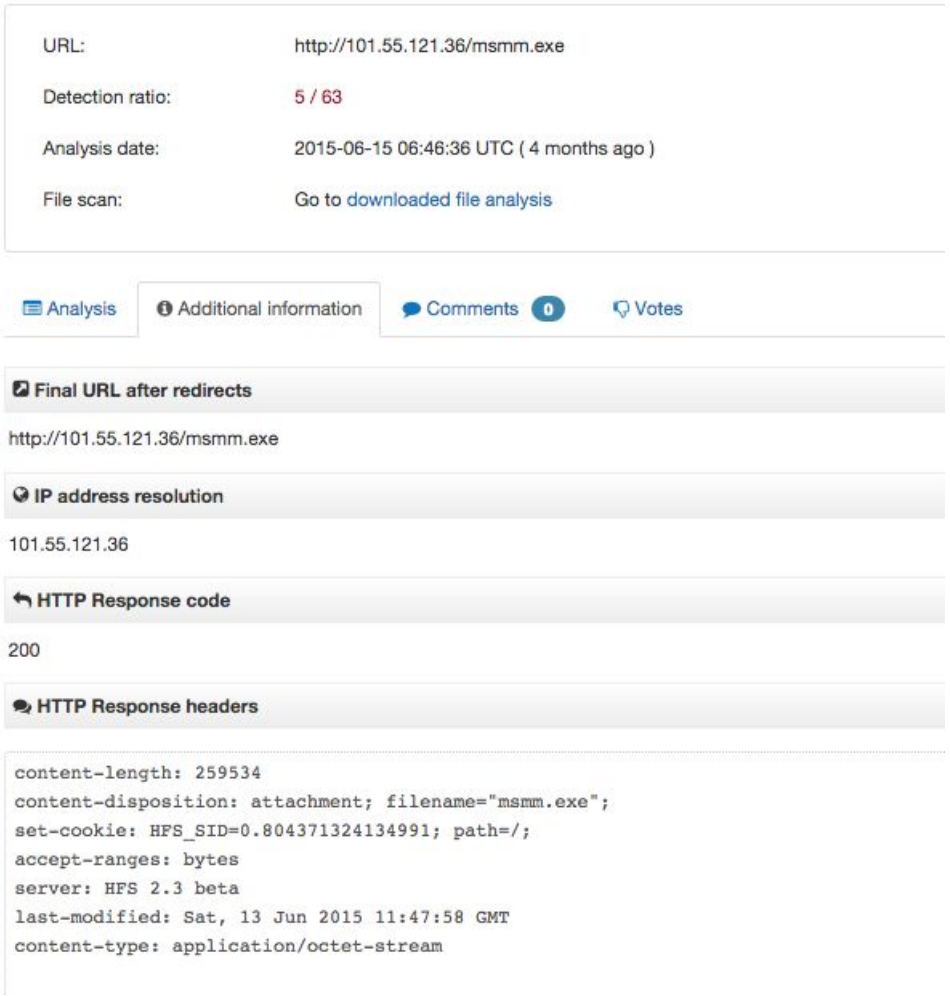
ATTRIBUTES

First Seen	2014-09-17 00:00:00
Last Seen	2015-10-10 15:54:09
Resolutions	134
Network	101.55.120.0/23
ASN	4766 (KIXS-AS-KR Korea Telecom)
Country	KR

Heatmap | Potential Malware 1

Source	Sample
virustotal	5b1430f955c0089dca797c3250edb71f18969c3321b5eac2139b7e42ae818cac

Level 1?!



URL: http://101.55.121.36/msmm.exe

Detection ratio: 5 / 63

Analysis date: 2015-06-15 06:46:36 UTC (4 months ago)

File scan: Go to downloaded file analysis

Analysis | Additional information | Comments 0 | Votes

Final URL after redirects

http://101.55.121.36/msmm.exe

IP address resolution

101.55.121.36

HTTP Response code

200

HTTP Response headers

```
content-length: 259534
content-disposition: attachment; filename="msmm.exe";
set-cookie: HFS_SID=0.804371324134991; path=/;
accept-ranges: bytes
server: HFS 2.3 beta
last-modified: Sat, 13 Jun 2015 11:47:58 GMT
content-type: application/octet-stream
```

Detailed analysis from VirusTotal:

https://www.virustotal.com/en/file/5b1430f955c0089dca797c3250edb71f18969c3321b5eac2139b7e42ae818cac/analysis/1434349022/

Observation

- Hook over WH_KEYBOARD_LL with SetWindowsHook method
- Sending back the data to 101.55.121.36:1604

Case Study #2: DDoS attack against Popvote

A voting site held by The University of Hong Kong is under DDoS attack.

You could get more background information from the following presentation slide:

https://www.hkupop.hku.hk/chinese/resources/workshops/20140925/PopVote_Seminar_22sept2014_Jazz.pdf

Date	Attack Event	Outcome	POP's Response
14th	DDoS on DNS service provider CloudFlare	CloudFlare added service rate limit to the domain name (popvote.hk)	Add Amazon Route 53 as another DNS service provider
15th - 16th	More than 100 billion DNS requests sent to Amazon	Amazon stopped providing Route 53 (DNS) and CloudFront (CDN) services	
	UDomain under attack with the peak traffic at 10Gbps	Stop providing protection service by UDomain	Turn on protection service by CloudFlare (with limited service rate)

17th	DNS and NTP Reflected DDoS attacks with the peak traffic of 150Gbps.		Report the incidents to the Police
18th	(Ongoing DDoS attacks)		Announce to extend voting period and prepare to use paper ballots.
19th			Enroll CloudFlare's Project Galileo and get 4 dedicated name servers by CloudFlare

20th	300Gbps DDoS attack taking place before the voting:	Mitigate by CloudFlare: Transfer zone files to some DNS service providers, use Anycast to absorb bandwidth consumption attack and hard code DNS responses with major recursors, including Google Public DNS, OpenDNS and HK IPS.	Update Android application to minimize the dependence on cloud hosting, and monitor the system around the clock by the Incident Response Team
	Layer 3 DNS Reflection and NTP reflection attacks		
	Layer 4 attacks including 100 million SYN packets recorded per second		
	Layer 7 DNS flood with 128 Gbps DNS requests received without amplification		
	Large amount of random and non-existent sub-domain requests	Whitelist existent sub-domains at Google Public DNS	
20th	Top level domain, .hk, under attacks		

More …..

23rd	Fake emails to SMS service provider to request SMS usage report		

27th	Phishing websites found	Turn down by HKDNR	

Can you handle this kind of attack in your hometown? :)

Compared with ransom in DDOS case, they will leave their contact, QQ number and phone number to the victim to pay the money, there is no way to pay off the attack from Popvote.